CLAIMS

What is claimed is:

1. A method, comprising the computer-implemented steps of:

determining a user identifier associated with a network device that has caused a security event in a network;

causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users; and

configuring one or more security restrictions with respect to the selected network address.

2. A method as recited in Claim 1, further comprising the steps of:

receiving information identifying the security event in the network;

correlating the security event information with network user information to result in determining the user identifier associated with the network device.

3. A method as recited in Claim 1, wherein the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the step of causing the network device to receive a network address comprises resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP.

4. A method as recited in Claim 1, wherein the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the step of causing the network device to receive a network address comprises issuing a DHCP FORCE_RENEW message to the network device.

5. A method as recited in Claim 1, wherein the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the step of causing the network device to receive a network address comprises prompting the network device to request a new network address using DHCP.

6. A method as recited in Claim 1, wherein the network device uses dynamic host control protocol (DHCP) to obtain the network address, and wherein the step of causing the network device to receive a network address comprises waiting for expiration of a lease for a current network address of the network device.

7. A method as recited in Claim 1, wherein the step of causing the network device to receive a network address comprises the step of providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet.

8. A method as recited in Claim 7, further comprising the step of publishing information describing characteristics of the special IP subnet to network service providers.

9. A method as recited in Claim 1, wherein the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the selected network address.

10. A method as recited in Claim 1, wherein the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the selected network address.

11. A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller.

12. A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, and if not, removing the user from the elevated risk group.

13. A method as recited in Claim 1, further comprising the steps of determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated with a trusted customer of a network service provider.

14. A method, comprising the computer-implemented steps of:

receiving information identifying a security event in a network;

correlating the security event information with network user information to result in determining a network user associated with the network device.

placing the user in an elevated risk security group;

configuring one or more security restrictions with respect to the selected network address;

determining whether a malicious act caused the security event;

if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller;

if a malicious act did not cause the security event, then removing the user from the elevated risk group.

15. A method as recited in Claim 14, wherein placing the user identifier in an elevated risk security group further comprises the step of forcing the user to acquire a new network address from a specified group of network addresses that is reserved for users associated with elevated user risk;

16. A method as recited in Claim 15, wherein forcing the user to acquire a new network address comprises the steps of:

re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk;

performing any one of the steps of:

(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP;

(b) issuing a DHCP FORCE_RENEW message to the network device;

(c) prompting the network device to request a new network address using DHCP;

(d) waiting for expiration of a lease for a current network address of the network device.

17. A method as recited in Claim 14, wherein the step of configuring one or more security restrictions comprises the steps of:

modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the selected network address;

modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the selected network address.

18. A computer-readable medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

determining a user identifier associated with a network device that has caused a security event in a network;

causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users; and

configuring one or more security restrictions with respect to the selected network address.

19. An apparatus, comprising:

means for determining a user identifier associated with a network device that has caused a security event in a network;

means for causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users; and

means for configuring one or more security restrictions with respect to the selected network address.

20. An apparatus, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

determining a user identifier associated with a network device that has caused a security event in a network;

causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users; and

configuring one or more security restrictions with respect to the selected network address.